

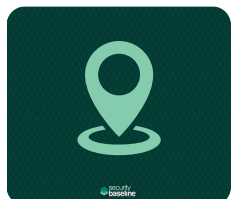
Gebaseerd op Microsoft 365-technologie, biedt deze baseline een gestandaardiseerde, schaalbare en toekomstbestendige aanpak voor informatiebeveiliging.

- ✓ Heldere licentiemodellen.
- ✓ Geen verrassingen in kosten of functionaliteit.
- ✓ Geen maandelijkse fee voor onderhoud en support.
- ✓ Eenvoudig beheer via 1 centraal portaal
- ✓ Snel op- en afschalen van gebruikers en apparaten.

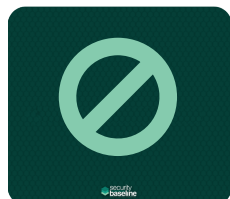
- ✔ Biedt templates om te voldoen aan eisen van o.a. NIS2, BIO en ISO27001.
- ✔ Automatische logging en rapportage van beveiligingsmaatregelen en afwijkingen.
- ✔ Beveiliging is geen losse laag, maar een integraal onderdeel van uw IT-structuur.



Wij handhaven strenge beveiligingsstandaarden en instellingen op de volgende kernonderdelen:



Toegang tot bedrijfsdata
alleen vanuit geografisch
specifieke gebieden of via
beheerde apparaten.



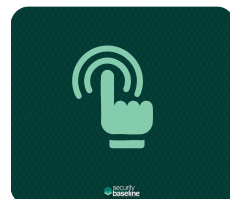
Blokkade van verouderde protocollen (POP3, IMAP).



Multi-Factor Authenticatie (MFA) voor alle accounts.



Beveiliging van bedrijfsdata op privéapparaten via MAM (Microsoft App Protection)



Bescherming tegen misconfiguraties en foutieve handelingen.

De TCA Security Baseline is ideaal voor organisaties die:

- ✔ Willen voldoen aan de modernste beveiligingsnormen.
- ✔ Flexibel willen werken, zonder concessies aan veiligheid.
- ✔ Zelf controle willen houden over gebruikersbeheer.
- ✔ Voor organisaties die het maximale willen halen uit het Microsoft Ecosysteem

- ✔ **Bedrijfseigen apparaten:** Volledig beheerd, compliant en altijd toegang tot apps en data.
- ✔ **Privéapparaten:** Veilige toegang via browser, met isolatie van bedrijfsdata en bescherming tegen datalekken.
- ✔ **Gebruik e-mail veilig op al uw apparaten, ook uw privé apparaten**



IT-afdelingen houden de regie, zonder de dagelijkse operatie te vertragen.



Selfservice blijft volledig beschikbaar: beheerders kunnen zelf accounts aanmaken, rechten toekennen, data delen en/of apparaten wissen/blokkeren.



Dankzij de onderliggende beveiligingslagen kunnen beheerders dit doen zonder risico op datalekken of misconfiguraties.



Het on- en offboarden van nieuwe medewerkers laat je met een gerust hart over aan je HR-afdeling.

Waarom is de implementatie van Security Baseline juist nu belangrijk?

Cyberdreigingen veranderen sneller dan ooit door technologie als AI. Voorkomen is beter dan genezen.

De Security Baseline valt binnen het standaard dienstenportfolio

MFA, protocolblokkades, apparaatbeheer, geografische toegangscontrole, 24/7 monitoring en meer.

Ja, als je maximale veiligheid, flexibiliteit en zelf in controle blijven belangrijk vindt.

Ja, met templates, logging en rapportages voor o.a. NIS2, BIO, ISO27001.vz z z zz ttv

Gartner:



*Cybersecurity trends waarop Security Baseline inspeelt.

